What is claimed is:

1. A method for providing authentication or identification services to a first user regarding a second user, the method comprising:

requesting a certificate corresponding to the second user from an authentication server;

returning the certificate corresponding to the second user;

requesting authentication of the certificate corresponding to the second user from a control program associated with the second user;

returning an authentication certificate from the control program associated with the second user; and

verifying authentication by comparing the authentication certificate corresponding to the second user and received from the control program associated with the second user with the certificate received from the authentication server.

2. The method according to claim 1, wherein the first user communicates with the second user through a media gateway.

3. The method according to claim 1, further comprising monitoring the communication between the first user and the second user so that the authentication server may notify the first user if the second user changes or becomes untrustworthy.

4. The method according to claim 1, wherein the requesting of the certificate corresponding to the second user from the authentication server, requesting authentication of the certificate corresponding to the second user and the verifying authentication is performed by a control program associated with the first user.

5. The method according to claim 1, wherein the first and second users are using client devices configured to communicate with each other and with the authentication server.

6. The method according to claim 5, wherein the client devices are smart phones.

7. The method according to claim 1, wherein the authentication server has authenticated an organization and the second user is a member of the authenticated organization.

8. The method according to claim 1, wherein verifying authentication determines a level of trust between the first user, the authentication server and the second user.

9. The method according to claim 8, wherein the level of trust is a value corresponding to the probability that the authentication certificate corresponding to the second user and received from the control program

associated with the second user is the same as the certificate received from the authentication server.

10. The method according to claim 1, wherein the authentication certificate corresponding to the second user and received from the control program associated with the second user includes a portion indicating the second user's identity.

11. A system for facilitating authentication services comprising:

an authentication server configured to provide an authentication certificate to a user of a first client device for authentication or identification of a user of a second client device, the first and second client devices being configured to communicate with each other and the authentication server, each of the first and second client devices including a user control program configured to communicate data to and from the authentication server, and a media gateway coupled to the authentication server and enabling communication of media data from the first and second client devices to the authentication server,

wherein, the user control program of the first client device is configured to receive a certificate corresponding to the user of the second client device and the authentication certificate from the authentication server and being configured to authenticate the user of the second client device by comparing the certificate corresponding to the second client device and the authentication certificate.

12. The system according to claim 11, wherein the authentication server is configured to monitor the communication between the first user and the second user.

13. The system according to claim 11, wherein the authentication server is configured to continuously monitor the communication between the first user and the second user so as to notify the first user if the second user changes or becomes untrustworthy.

14. The method according to claim 11, wherein the control program associated with the first user is configured to request the certificate corresponding to the second user from the authentication server, request authentication of the certificate corresponding to the second user and verify authentication.

15. The system according to claim 1, wherein the first and second users use client devices configured to communicate with each other and with the authentication server.

16. The system according to claim 15, wherein the client devices are smart phones.

17. The system according to claim 11, wherein the authentication server has authenticated an organization and the second user is a member of the authenticated organization.

18. The system according to claim 14, wherein verifying authentication determines a level of trust between the first user, the authentication server and the second user.

19. The system according to claim 18, wherein the level of trust is a value corresponding to the probability that the authentication certificate corresponding to the second user and received from the control program associated with the second user is the same as the certificate received from the authentication server.

20. The system according to claim 11, wherein the authentication certificate corresponding to the second user and received from the control program associated with the second user includes a portion indicating the second user's identity.

21. A method comprising:

receiving biometric user input;

receiving reference biometric user input that has been authenticated by an authentication server; and

comparing the biometric user input with the reference biometric user input;

determining a probability based upon the comparison between the biometric user input and the reference biometric user input; and

authenticating an end user based upon the determined probability.

22. The method according to claim 21, wherein the first user communicates with the second user through a media gateway.

23. The method according to claim 21, further comprising monitoring the communication between the first user and the second user so that the authentication server may notify the first user if the second user changes or becomes untrustworthy.

24. The method according to claim 21, wherein the requesting of the certificate corresponding to the second user from the authentication server, requesting authentication of the certificate corresponding to the second user and the verifying authentication is performed by a control program associated with the first user.

25. The method according to claim 21, wherein the first and second users are using client devices configured to communicate with each other and with the authentication server.

26. The method according to claim 25, wherein the client devices are smart phones.

27. The method according to claim 21, wherein the authentication server has authenticated an organization and the second user is a member of the authenticated organization.

28. The method according to claim 21, wherein verifying authentication determines a level of trust between the first user, the authentication server and the second user.

29. The method according to claim 28, wherein the level of trust is a value corresponding to the probability that the authentication certificate corresponding to the second user and received from the control program associated with the second user is the same as the certificate received from the authentication server.

30. The method according to claim 21, wherein the authentication certificate corresponding to the second user and received from the control program associated with the second user includes a portion indicating the second user's identity.

31. A method comprising:

receiving biometric user input;

receiving reference biometric user input that has been authenticated by an authentication server; and

comparing the biometric user input with the reference biometric user input;

determining a level of trust based on the comparison between the user input and the reference biometric user input; and

authenticating an end user based upon the level of trust.

32. The method according to claim 31, wherein the first user communicates with the second user through a media gateway.

33. The method according to claim 31, further comprising monitoring the communication between the first user and the second user so that the authentication server may notify the first user if the second user changes or becomes untrustworthy.

34. The method according to claim 31, wherein the requesting of the certificate corresponding to the second user from the authentication server, requesting authentication of the certificate corresponding to the second user and the verifying authentication is performed by a control program associated with the first user.

35. The method according to claim 31, wherein the first and second users are using client devices configured to communicate with each other and with the authentication server.

36. The method according to claim 35, wherein the client devices are smart phones.

37. The method according to claim 31, wherein the authentication server has authenticated an organization and the second user is a member of the authenticated organization.

38. The method according to claim 31, wherein verifying authentication determines a level of trust between the first user, the authentication server and the second user.

39. The method according to claim 38, wherein the level of trust is a value corresponding to the probability that the authentication certificate corresponding to the second user and received from the control program associated with the second user is the same as the certificate received from the authentication server.

40. The method according to claim 31, wherein the authentication certificate corresponding to the second user and received from the control

program associated with the second user includes a portion indicating the second user's identity.

41. An end user control module configured to facilitate authentication services comprising:

a user interface configured to receive biometric user input;

a media gateway interface configured to receive reference biometric user input through a media gateway;

an authentication application configured to authenticate an end user by comparing the biometric user input and the reference biometric user input and determining a level of trust representing the probability that the biometric user input corresponds to the reference biometric user input.

42. An end user control module according to claim 41, wherein the media gateway is coupled to an authentication server.

43. An end user control module according to claim 41, wherein the authentication application is a biometric service provider including software or processing algorithm.

44. An end user control module according to claim 41, further comprising a dialog system configured to interact with an end-user to collect biometric information from the end-user.

45. An end user control module according to claim 44, wherein the dialog system collects speech or voice data from the end-user and uses the speech or voice data as raw data for constructing a biometric identification record.

46. An end user control module according to claim 44, wherein the biometric information collected from the end-user includes voice characteristics, fingerprints, hand geometry, facial geometry or movement, retina scans or iris scans.

47. An end user control module according to claim 41, wherein the end user control module is a smart phone.